

North Carolina Security Breach Reporting Form
Pursuant to the Identity Theft Protection Act of 2005

*Indicated a mandatory field

*Name of the Company or Government Agency owning or licensing information affected by the entity experiencing breach:

WILBRAHAM, LAWLER & BUDA, PC

Entity Type: GENERAL BUSINESS

Address:

Apt/Suite/Building:

City:

State:

Zip Code:

Telephone:

Fax:

Email:

*Date Security breach Reporting Form Submitted: 12/31/2017

Is this notice a supplement to a previously filed NO

Security Breach:

*Date the Security Breach was discovered: 09/19/2017

Breach Type: HACKERS/ UNAUTHORIZED ACCESS

*Estimated number of affected individuals: 134

*Estimated number of NC residents affected: 134

Name of company or government agency maintaining or possessing information that was the subject of the Security Breach, if the agency that experienced the Security Breach is not the same entity as the agency reporting the Security Breach (pursuant to N.C.G.S. 75-65(b))

Describe the
circumstances
surrounding the
Security Breach:

AG ENTERED WEB FORM

POSSESSION OF WILBRAHAM, LAWLER & BUBA, P.C. ("WLB") WAS POTENTIALLY BREACHED. WLB IS A LAW FIRM WHICH PRIMARILY REPRESENTS DEFENDANTS IN ASBESTOS, WORKERS' COMPENSATION, AND OTHER TYPES OF PERSONAL INJURY AND/OR PROPERTY DAMAGE LITIGATION, THOUGH IT HANDLES OTHER TYPES OF MATTERS AS WELL. IN THE COURSE OF ITS WORK ONE OR MORE LITIGATION MATTERS, WLB RECEIVED PERSONAL INFORMATION REGARDING RESIDENTS OF NORTH CAROLINA. WLB WAS RECENTLY THE SUBJECT OF A "RANSOMWARE" ATTACK, WHICH RESULTED IN THE ENCRYPTION OF ALL OF THE DATA ON ITS SERVERS. LAW ENFORCEMENT WAS NOTIFIED OF THE ATTACK, AND WLB HAS CONDUCTED AN INTERNAL REVIEW OF THE MATTER. WHILE IT DOES NOT APPEAR THAT THEFT OF PERSONAL INFORMATION WAS THE FOCUS OF THE ATTACK, ON OR ABOUT SEPTEMBER 19, 2017, WLB BECAME AWARE OF ACTIVITY CONSISTENT WITH THE POTENTIAL ACCESS OF SUCH INFORMATION ON ITS SYSTEMS. DEPENDING ON THE SPECIFICS OF A GIVEN SITUATION, THE TYPES OF PERSONAL INFORMATION OF NORTH CAROLINA RESIDENTS IN WLB'S SYSTEMS MAY HAVE

INCLUDED NAMES AND SOME COMBINATION OF THE FOLLOWING:
SOCIAL SECURITY NUMBERS, ADDRESSES, MEDICAL INFORMATION,
EMPLOYMENT INFORMATION, DRIVER'S LICENSE INFORMATION,
SETTLEMENT DOCUMENTATION AND DATES OF BIRTH. PLEASE
BE ADVISED THAT CREDIT CARD OR BANK ACCOUNT INFORMATION
WAS NOT PROVIDED TO WLB.

Information Type: MEDICAL INFORMATION
SSN

*Regarding information
breached, if
electronic, was the
information
protected in some
manner: YES

If YES, please
describe the
security measures
protecting the
information:

*Describe any measures taken to prevent a similar Security Breach from occurring in the future: WLB TAKES THE PROTECTION OF PERSONAL INFORMATION SERIOUSLY AND IS TAKING STEPS TO PREVENT ANY SIMILAR OCCURRENCE IN THE FUTURE THROUGH THE CONSTRUCTION OF AN ENTIRELY NEW COMPUTER SYSTEM. FURTHERMORE, WHILE THE INVESTIGATION TO DATE DOES NOT CONFIRM WHETHER ANY NORTH CAROLINA RESIDENT'S PERSONAL INFORMATION WAS ACCESSED, ON NOVEMBER 3, 2017, WLB SENT A NOTICE TO THE 134 IMPACTED NORTH CAROLINA RESIDENTS.

*Date affected NC residents were/will be notified: 11/03/2017

Describe the circumstances surrounding the delay in notifying affected NC residents pursuant to N.C.G.S. 75-65 (a) and (c):

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. 75-65(c), please attach or mail the written request or the contemporaneous memorandum.

How NC residents were/will be WRITTEN NOTICE

notified? (pursuant
to N.C.G.S. 75-65
(e)):

Please note if the business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000) or that the affected class of subject persons to be notified exceeds 500,000, or if the business does not have sufficient contact information or consent to satisfy subdivisions (1), (2) , or (3) of this subsection, for only those affected persons without sufficient contact information or consent, or if the business is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following:

- Email notice when the business has an electronic mail address for the subject persons
- Conspicuous posting of the notice on the Web site page of the business, if one is maintained
- Notification to major statewide media

Please attach a copy of the notice if in written form or a copy of any scripted notice if in telephonic form.

Contact Information SAME AS ABOVE
Affiliation with entity
experiencing breach:

Organization Name:

Prefix:

*First Name: BRADY

Middle Name:

*Last Name: GREEN

Suffix:

Title:

Address:

Apt/Suite/building:

City:

State:

Zip Code:

*Telephone: (855) 260-2771 Fax:

Email: CONSUMER@NCDOJ.GOV

☐ **PHILADELPHIA OFFICE**
1818 MARKET ST. SUITE 3100
PHILADELPHIA, PA 19103-3631
TEL: 215.564.4141
FAX: 215.564.4385

☐ **PITTSBURGH OFFICE**
603 STANWIX STREET
TWO GATEWAY CENTER, 17 N.
PITTSBURGH, PA 15222
TEL: 412.255.0500
FAX: 412.255.0505

☐ **WEST VIRGINIA OFFICE**
25 11th STREET
WHEELING, WV 26003
TEL: 304.905.9463
FAX: 304.905.1194

WILBRAHAM LAWLER & BUBA

A Professional Corporation

www.wlbdeflaw.com

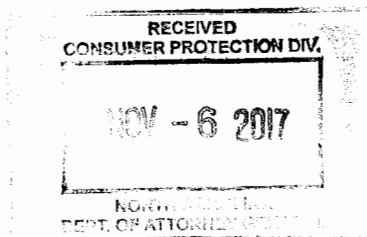
☐ **NEW JERSEY OFFICE**
30 WASHINGTON AVE., SUITE B3
HADDONFIELD, NJ 08033-3341
TEL: 856.795.4422
FAX: 856.795.4699

☐ **NEW YORK OFFICE**
140 BROADWAY, 46TH FLOOR
NEW YORK, NY 10005
TEL: 212.858.7575
FAX: 212.943.9246

☐ **DELAWARE OFFICE**
901 MARKET STREET
SUITE 810
WILMINGTON, DE 19801
TEL: 302.421.9935
FAX: 302.421.9955

November 3, 2017

Consumer Protection Division
Attorney General's Office
Mail Service Center 9001
Raleigh, NC 27699-9001



To Whom It May Concern:

Pursuant to N.C. Gen. Stat. § 75-65, this letter is to inform you that data in the possession of Wilbraham, Lawler & Bubba, P.C. ("WLB") was potentially breached. WLB is a law firm which primarily represents defendants in asbestos, workers' compensation, and other types of personal injury and/or property damage litigation, though it handles other types of matters as well. In the course of its work on one or more litigation matters, WLB received personal information regarding residents of North Carolina. WLB was recently the subject of a "ransomware" attack, which resulted in the encryption of all of the data on its servers. Law enforcement was notified of the attack, and WLB has conducted an internal review of the matter. While it does not appear that theft of personal information was the focus of the attack, on or about September 19, 2017, WLB became aware of activity consistent with the potential access of such information on its systems.

Depending on the specifics of a given situation, the types of personal information of North Carolina residents in WLB's systems may have included names and some combination of the following: Social Security numbers, addresses, medical information, employment information, driver's license information, settlement documentation and dates of birth. Please be advised that credit card or bank account information was not provided to WLB.

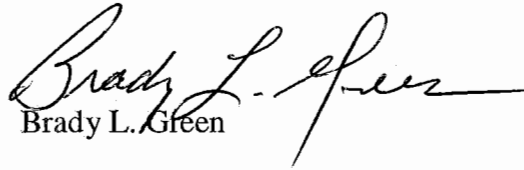
WLB takes the protection of personal information seriously and is taking steps to prevent any similar occurrence in the future through the construction of an entirely new computer system. Furthermore, while the investigation to date does not confirm whether any North Carolina resident's personal information was accessed, on November 3, 2017, WLB sent a notice to the 134 impacted North Carolina residents. A copy of this notice is enclosed.

Additionally, WLB has agreed to make identity protection services available to the impacted North Carolina residents for one year free of charge through AllClear ID.

WLB believes that this letter is compliant with the notice requirements listed in N.C. Gen. Stat. § 75-65. If, however, you require additional information or documentation, please do not hesitate to contact WLB's counsel, Christopher Nucifora, Esq. of Kaufman, Dolowich & Voluck, LLP at 201-708-8207. Thank you for your time and attention.

Very truly yours,

Wilbraham, Lawler & Buba, P.C.


Brady L. Green



Processing Center • P.O. BOX 141578 • Austin, TX 78714



00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

November 3, 2017

NOTICE OF DATA BREACH

Dear John Sample,

We are writing to inform you of an incident that may have involved your personal information.

What Happened

Wilbraham, Lawler & Buba, P.C. ("WLB") is a law firm which represents defendants in asbestos, workers' compensation and other types of personal injury and property damage litigation. In the course of such an action, we received personal information regarding you. WLB was recently the subject of a "ransomware" attack, which resulted in the encryption of all of the data on our servers. Law enforcement was notified of the attack, and WLB has conducted an internal review of the matter. While it does not appear that theft of personal information was the focus of the attack, on or about September 19, 2017 we became aware of activity consistent with the potential access of such information on our systems.

What Information Was Involved

Depending on the specifics of a given situation, the types of personal information in our systems may have included names and some combination of the following: Social Security numbers, addresses, medical information, employment information, driver's license information, settlement documentation and dates of birth. Please be advised that your credit card or bank account information was not provided to us.

What We Are Doing

WLB takes the protection of your personal information seriously and is taking steps to prevent any similar occurrence in the future through the construction of an entirely new computer system. Furthermore, notice of the breach of our system is being provided pursuant to relevant notification statutes.

What You Can Do?

While the investigation to date does not confirm whether your personal information was accessed, we want to make you aware of steps you may take to guard against identity theft or fraud. Please review the enclosed Information about Identity Theft Protection.

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-260-2771 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.



01-03-1-00

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical or employment fraud against children by searching thousands of public databases for use of your child's information. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-260-2771 using the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

For More Information

WLB and all of its employees apologize for any inconvenience or concern that this matter may cause you. If you have any further questions, please feel free to contact us at 1-855-260-2771, Monday through Saturday, 8:00 a.m. to 8:00 p.m. Central Time, and we will be happy to assist you.

Sincerely,

Wilbraham, Lawler & Buba, P.C.

Information about Identity Theft Prevention

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax, P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com

Experian, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com

TransUnion, P.O. Box 6790, Fullerton, CA 92834-6790, 1-800-916-8800, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, which is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center

600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division

200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division

9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

For residents of Rhode Island: You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General

Rhode Island Office of the Attorney General, Consumer Protection Unit

150 South Main Street, Providence, RI 02903, 401-274-4400, www.riag.ri.gov

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider or plan and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider or plan, to serve as a baseline.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.



02-03-1

Equifax: 1-800-525-6285, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, www.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian, P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion, Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790, www.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

For residents of Massachusetts: Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;

8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

